

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
WESTERN DIVISION**

ExactLogix, Inc. d/b/a Acculynx.com,

Plaintiff,

v.

JobProgress, LLC, Double D
Construction, LLC, Dennis A. Darrow,
and David Buzzelli,

Defendants.

Case No. 3:18-cv-50213

Honorable Iain D. Johnston

MEMORANDUM OPINION AND ORDER

Plaintiff ExactLogix, doing business as AccuLynx.com, brings this action against JobProgress, LLC, Double D Construction, LLC, Dennis A. Darrow, and David Buzzelli (“Defendants”). It claims violations of the Computer Fraud and Abuse Act (CFAA) and the Illinois Trade Secret Act, (ITSA), breach of contract, fraud, unjust enrichment, conspiracy, and common law unfair competition. Before the Court are cross motions for summary judgment. For the reasons below, Plaintiff’s motion for partial summary judgment [157] is denied. Defendants’ motion for summary judgment [123] is granted in part and denied in part.

I. Background

The following facts are taken from the statements of undisputed facts filed by both sides as part of the summary judgment motion briefing, and to some extent,

from the depositions directly. At issue are two competing software programs that aid construction companies with various administrative and job-tracking tasks. Dkt. 171, ¶ 5. Plaintiff's software, Acculynx, came first. Defendant Double D Construction—which is owned by Defendant Dennis Darrow—was a subscriber to that software. *Id.* ¶ 3. The gist of the complaint is that the Defendants used Double D Construction's access to Acculynx to build a competing product, JobProgress, and are now in direct competition with Plaintiff's software. *Id.* ¶ 2; Dkt. 178, ¶ 43. Dennis Darrow hired David Buzzelli to work in sales at Double D Construction in April 2013. Dkt. 178, ¶ 18. They then started JobProgress, LLC together. Dkt. 171, ¶ 2; David Buzzelli became the Managing Partner of JobProgress, LLC, while Dennis Darrow became the President of JobProgress, LLC. *Id.* ¶¶ 3–5.

Specifically, Plaintiff alleges that Defendants and their consultants used their Acculynx customer login credentials to build a competing product based on the functionality of Acculynx. Defendants, however, contend that they merely set out to develop a better product and used their Acculynx customer login credentials to migrate their information from Acculynx to the new system. The factual assertions in this case are numerous, as are the disputes.

Plaintiff demonstrates its software, Acculynx, at trade shows, in online presentations, and in other demonstrations to win over prospective customers. *Id.* ¶ 12. They show depictions of parts of the software on large screens at these trade shows, and Plaintiff instructs its Acculynx sales representatives to give follow-up presentations if any prospective customer has additional questions. *Id.* ¶¶ 13–14.

These sessions are not bound by confidentiality agreements. *Id.* ¶ 17. Once someone becomes a customer, however, they are contractually bound by a Master Subscription Agreement that includes confidentiality provisions and a non-compete clause. That customer then may have multiple users that operate under the same subscription agreement. Though they operate under the Master Subscription Agreement, each user must reaffirm their consent to the terms and conditions of use each time they login to the Acculynx software.¹ Dkt. 178, ¶ 11.

Though the reason is disputed, Double D Construction became a subscribing customer to the Acculynx software in 2013. *Id.* ¶¶ 17–18. Plaintiff sees this as part of larger conspiracy, but whatever the reason, David Buzzelli then hired Logiciel, a software development company in India, to develop the JobProgress software—eventually spending nearly \$300,000 on development services with Logiciel. Dkt. 175, ¶ 8. Defendants do not dispute that they shared their Acculynx login credentials with Logiciel and that Logiciel used those credentials to access Acculynx beginning in September 2014.² Dkt. 178, ¶ 32. They do, however, dispute the reason for that sharing. Although Plaintiff sees it as part of a larger conspiracy that resulted in Logiciel using Acculynx login credentials to copy the software, Defendants claim the Logiciel consultants merely needed the login credentials to migrate Defendants’ information to the new JobProgress software.

¹ This was done in a conspicuous manner. Defendants did not dispute that the Acculynx login screen states that logging in implies assent to the “terms and conditions,” that those words were set off in blue text, and that the text used a hyperlink to direct customers to the full terms and conditions. Dkt. 178, ¶ 13.

² From September 2014 to September 2015 Logiciel used Double D Construction’s login credentials to access the Acculynx software 228 times. Dkt. 178, ¶ 39.

Still, Logiciel employees explained that having the Acculynx login credentials made it easier to understand how Defendants wanted JobProgress to be developed. *Id.* ¶ 29. These logins were all recorded. Plaintiff notes that it maintains logs of all access attempts and that those logs are monitored infrequently at the request of customers or on suspicion of nefarious activity. Dkt. 171, ¶ 10. Defendant characterizes Plaintiff's review of its logging system as quarterly and that it would have known "immediately when it saw logins from India," which is where the Logiciel consultants worked. *Id.* But this language is not supported by the cited deposition, which explicitly states that the reviews are done infrequently at the customer's request. At a minimum, Defendants' characterization of the testimony is not a reasonable inference of fact and is not accepted. *Hernandez v. Foster*, 657 F.3d 463, 473 (7th Cir. 2011).

When David Buzzelli signed Double D Construction up for Acculynx's software, he signed a Master Subscription Agreement and a Training Agreement. Dkt. 178, ¶¶ 10, 14, 17. These agreements were signed before JobProgress, LLC was formed. Dkt. 171, ¶ 35. The agreements made Double D Construction a licensee of the Acculynx software, which permitted Double D Construction to create multiple user accounts for its employees and agents. *Id.* ¶ 52. Acculynx could then bill Double D Construction for each user that it created. *Id.* Still, Defendants shared their login credentials with the Logiciel consultants instead of creating separate credentials for them. No one disputes that the login credentials were shared. Furthermore, no one disputes that this is the extent of the network security issues.

No one is accused of any further malicious cyber activity and Plaintiff does not allege any physical systems damage, corruption of data, or service interruption. *Id.* ¶ 9.

Defendants do not dispute that David Buzzelli and Dennis Darrow both logged into the Acculynx system and agreed to the terms and conditions. Dkt. 178, ¶ 14. Those terms and conditions included a provision, in all caps, that stated, “By accessing or using all or any portion of the software, you are agreeing to be bound by the terms of this agreement If you do not agree to the terms of this agreement . . . do not access or use the software.” *Id.* ¶ 16. The terms then included provisions banning the sharing of login information and requiring that subscribers ensure Acculynx access is only afforded to those individuals for whom license fees are paid. *Id.* (quoting § 1.3 and § 1.4.4). The terms and conditions also prohibited licensees from reverse engineering Acculynx or creating derivative works. *Id.* (quoting § 1.4.1). They also included a provision preventing licensees from making “the Software available to any third party other than Users.” *Id.* (quoting § 1.4.3). The terms and conditions also noted that “the Software and all of its components are trade secrets.” *Id.* (quoting § 1.5). If Acculynx discovered any sharing of login credentials, the terms and conditions allowed for retroactive and automatic billing of the credit card on file. *Id.* (quoting § 2.7).

After Buzzelli subscribed to Acculynx on behalf of Double D Construction, Dennis Darrow expressed dissatisfaction with Acculynx and the two agreed to create their own product. Dkt. 174, ¶ 18. They wanted to create a “streamlined

efficient version of what Acculynx offers.” *Id.* At times, they proposed names for their new software that were similar to Acculynx—names like Accuwork, AccuBench, and AccuJob. *Id.* They finally settled on JobProgress, which also happens to be the name of one of the Acculynx screens. *Id.* They proceeded to create JobProgress in Acculynx’s likeness, at least in part. In conversations with the Logiciel consultants, Buzzelli noted that Defendants had access to Acculynx. Furthermore, he sent those consultants a link to software used to clone websites. *Id.* ¶¶ 19–20. In response, Defendants do not dispute those facts. They do contend, however, that JobProgress was developed from scratch over the course of nine months, at significant cost to them, and any similarities in function with Acculynx are similarities shared with other competing software on the market. *Id.* ¶ 19.

After contracting with Logiciel, Defendant Buzzelli appears to have taken screenshots of Acculynx and shared those screenshots with the consultants as part of the effort to create JobProgress—the reasonable inference being that he wanted JobProgress to be developed to look similar to Acculynx. Although not disputing that, Defendants respond that those screenshots of the Acculynx software that were shared with the Logiciel consultants were public information because they are available either through simple Google searches or through one of the Acculynx demonstrations, or both. *Id.* ¶ 22. Ajay Sharma—from Logiciel—noted that these screenshots helped him better understand how Buzzelli wanted him to create JobProgress. *Id.* ¶ 25. Defendants even recorded an Acculynx webinar that showed licensed customers a new beta version of the dashboard. Defendants then shared

that recording with the Logiciel consultants for them to use as a benchmark and to possibly incorporate those new ideas into the JobProgress software. *Id.* ¶¶ 34–35.

Though disputes exist, at a minimum, the facts show that Defendants spent nine months building their competing software, that they built it using Acculynx screenshots as inspiration, and that they shared their Acculynx login credentials with their third-party consultants. Still, Defendants dispute the reason they shared the login credentials with the Logiciel consultants. After JobProgress, LLC was formed and began offering its software to customers in 2015, at least 134 Acculynx customers switched and became customers of JobProgress. Dkt. 178, ¶ 50.

Plaintiff ExactLogix, doing business as Acculynx.com, now brings this action claiming eight different counts against Defendants. Plaintiff has moved for summary judgment on its claims under the Computer Fraud and Abuse Act, breach of contract, and conspiracy to commit both of those violations. Dkt. 159, at 1. Defendants move the Court for summary judgment as to all claims against them. Dkt. 146, at 7. Plaintiff concedes that summary judgment in favor of Defendants is appropriate on Plaintiff's claim under the implied covenant of good faith and fair dealing, but it contests summary judgment on the remaining claims. Dkt. 167, at 14.

II. Discussion

Both sides have moved the Court for summary judgment, though Plaintiff's motion asks only for judgment on three counts. At this stage, the party moving for

summary judgment has the burden to show that “no genuine dispute as to any material fact” exists and that they are “entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a); *Duberville v. WMG, Inc.*, No. 13 C 02061, 2015 U.S. Dist. LEXIS 4157, at *14–15 (N.D. Ill. Jan. 13, 2015). The Court must construe the “evidence and all reasonable inferences in favor of the party against whom the motion under consideration is made.” *Rickher v. Home Depot, Inc.*, 535 F.3d 661, 664 (7th Cir. 2008). The parties do not dispute that Illinois contract law applies. Dkt. 178, at 17.

A. Computer Fraud and Abuse Act

Plaintiff’s first count claims that Defendants violated the Computer Fraud and Abuse Act (CFAA) by sharing their login credentials with outside consultants. Dkt. 100, ¶¶ 33–34, 49–55. Defendants argue that they are entitled to summary judgment on the CFAA claim because it is time barred and because Plaintiff both has not alleged damage and cannot show loss. Dkt. 146, at 14–18. For the reasons below, Defendants’ summary judgment motion on the CFAA claim is denied. Plaintiff’s motion on merits of the same claim is also denied.

1. Statute of Limitations

Congress originally passed the CFAA in 1984 to protect against hackers’ attempts to disrupt and destroy computer systems or steal information. *United States v. Nosal*, 844 F.3d 1024, 1032 (9th Cir. 2016). Congress expanded the statute two years later to include protections for private computers. *Id.* Although the CFAA is mostly a criminal statute, it provides for a private right of action for anyone that

has suffered damage *or* loss of at least \$5,000. *Pascal Pour Elle, Ltd. v. Jin*, 75 F. Supp. 3d 782, 790 (N.D. Ill. 2014). But this private right of action is subject to a statutorily defined limitations period. The CFAA provides that “[n]o action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the *damage*.” 18 U.S.C. § 1030(g) (emphasis added).

In the CFAA, Congress differentiated between damage and loss, and defined them expressly. Damage “means any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). Loss refers to “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11).

Defendants contend that the CFAA claim is time barred because more than two years have passed since any damage occurred and because the statute of limitations accrues from the discovery of damage and not from the discovery of loss. Plaintiff responds (1) that the discovery rule applies to discovery of either damage or loss, (2) that the statute of limitations should be equitably tolled, and (3) that Defendants have failed to show that they did not violate the statute in the two years preceding the date this action was filed. Dkt. 167, at 14–15.

Defendants argue that the two-year limitations period begins at least on discovery of the alleged damage—as that word is statutorily defined. In support, Defendants point out that Congress omitted the term loss when it could have included it in the sentence describing the limitations period, and therefore, manifested an intention to begin the limitations timer on discovery of the damage. Dkt. 146, at 15. Plaintiff responds that the law is not clear on that point and the statute could be read to mean any damages—whether from the statutorily defined damage or loss. Dkt. 167, at 15. But Congress expressly defined those two words and chose to only use one when setting the boundaries of the private right of action. And courts can assume that “Congress acts intentionally when it omits language included elsewhere.” *Dep’t of Homeland Sec. v. MacLean*, 574 U.S. 383, 392 (2015). The plain language is not ambiguous. Suit must be brought within two years “of the act complained of or the date of the discovery of the damage.” 18 U.S.C. § 1030(g). Given a lack of ambiguity, this Court will not read the word loss into the statute.

Furthermore, Plaintiff’s interpretation of the statute of limitations would create a reality that Congress likely did not intend. *Trans Alaska Pipeline Rate Cases*, 436 U.S. 631, 643 (1978) (explaining that statutes should be read to avoid absurd results). The statutory definition for loss is broad. It includes the cost of responding to alleged damage, of repairing computer systems, and it includes lost revenue. 18 U.S.C. § 1030(e)(11). These are losses that could be felt for a considerable amount of time after the plaintiff has been made aware of the violation. Indeed, many of these losses would necessarily have to come after

plaintiffs became aware of the occurrence of damage because they are losses incurred by responding to that damage.

As discussed below, this would stretch the limitations period too far and would seemingly empower plaintiffs beyond the rationale underpinning statutes of limitation. If the statute of limitations ran from the occurrence of loss, then plaintiffs would have control over the limitations period. Plaintiffs could simply spend more money investigating the alleged violation, as such expenses fall within the definition of loss—thereby extending the limitations period, which is supposed to act as a check on plaintiffs.

In support of its claim, Plaintiff cites to *Halperin v. Int'l Web Servs.*, 70 F. Supp. 3d 893, 899 (N.D. Ill. 2014). But that case did not discuss the CFAA's limitations period and is not persuasive. On the other hand, Defendants' citation to *Kluber Skahan & Associates v. Cordogan, Clark & Associates*, No. 08-cv-1529, 2009 U.S. Dist. LEXIS 14527 (N.D. Ill. Feb. 25, 2009) is persuasive. There, the court was asked to decide this exact issue. That court noted, as does this one, that the plain language of the statute forecloses the argument that the statute of limitations runs from the discovery of loss. *Id.* at *27. The *Kluber* court went on to note that “[l]osses are monetary harms attenuated from the underlying concern of the Act: damage to data. Extending the scope of liability by extending the CFAA’s injury-discovery limitation to include a two-year discovery of loss limitation attenuates liability under the Act to its breaking point.” *Id.*

Given the general principle that harms accrue for the purpose of statutes of limitation once the victim is on notice that a violation has occurred,³ the reasonable interpretation of the CFAA remains consistent with the plain language. Losses stem from alleged damage. Although losses are recoverable under the CFAA, the discovery of damage is what places plaintiffs on notice that they must exercise their right to legal redress or lose it. Without express language from Congress, the Court declines to read the statute in another way. Plaintiff's claim accrued on the date of the act complained of or on discovery of any damage, and its CFAA claim is barred if not commenced within two years of either of these dates. *Accord Sewell v.*

Bernardin, 795 F.3d 337, 340 (2nd Cir. 2015) ("The CFAA's statute of limitations began to run when Sewell learned that the integrity of her account had impaired."); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (explaining that the discovery provision that can "lengthen the statute of limitations applies only to the discovery of damage, not loss").

Although not mentioned in the plain text of the statute, some courts have analyzed the CFAA's statute of limitations date using an objective test. These courts ask when the plaintiff "knew or reasonably should have known that he or she was wrongfully injured." *Navistar, Inc. v. New Baltimore Garage, Inc.*, No. 11-cv-6269, 2012 U.S. Dist. LEXIS 134369, at *24 (N.D. Ill. Sept. 20, 2012) (quoting

³ "[I]t is a general principle of federal law that the determination of when a cause of action accrues is an objective test, i.e. when the plaintiff discovered or should have discovered in the exercise of reasonable diligence the facts giving rise to the claim." *Havenick v. Network Express*, 981 F. Supp. 480, 513 (E.D. Mich. 1997) (collecting cases); *see also Baxter v. State Teacher's Ret. Sys.*, 18 Cal. App. 5th 340, 360 (Cal. Ct. App. 2017) (noting "the principle that 'statutes of limitations are intended to run against those who fail to exercise reasonable care in the protection and enforcement of their rights'" (quoting *Saliter v. Pierce Bros. Mortuaries*, 146 Cal. Rptr. 271, 274 (Cal. Ct. App. 1978))).

Horbach v. Kaczmarek, 288 F.3d 969, 973 (7th Cir. 2002) (applying the objective test in another context)). Stated differently, they determine the date of discovery or the date on which the plaintiff should have discovered the damage. *Id.*; *see also Ashcroft v. Randel*, 391 F. Supp. 2d 1214, 1219–20 (N.D. Ga. 2005) (applying an objective test to the limitations period in the *Bivens* context and the CFAA claim).

Still, on summary judgment, the Court can only make determinations when no reasonable disputes of material fact exist. Here, that is not the case. Defendants argue that Plaintiff's logging system would have known "immediately" if anyone other than authorized users logged into the system. Dkt. 146, at 16. But that claim appears to be inconsistent with the cited deposition, as Plaintiff points out.⁴ Dkt. 167, at 18. Defendants cite to Mr. McLeod's deposition, but he states that the logs are checked infrequently, McLeod Dep. 29:7, and that they are kept in case a customer has concerns, *id.* at 29:14–20. He also testified that he performed his investigation into Defendants' logins from India after learning of potential nefarious activity in 2018. *Id.* at 9:16–22.

Although nothing in the deposition supports Defendants' assertion that Plaintiff would have known about nefarious activity immediately in 2014 or 2015, Mr. McLeod also testified that "from time to time, we'll just take a look and make sure that there isn't any odd access going on in our system." McLeod Dep. 33:12–14. He went on to estimate that such checks are done quarterly. *Id.* at 34:7–14. Thus, a genuine dispute exists regarding the date on which the alleged CFAA violation was

⁴ Specifically, Plaintiff asserts that they review the logs infrequently at a customer's request or "upon learning something nefarious." Dkt. 167, at 18.

discovered or should have been discovered by reviewing logs. Therefore, summary judgment on the CFAA statute of limitations question is denied.

2. Can Plaintiff show loss under the CFAA?

Defendants next urge the Court that it is entitled to summary judgment on the CFAA claim because Plaintiff cannot show that it suffered loss as defined by the CFAA. The crux of Defendants' argument is that CFAA loss results from CFAA damage. Although Plaintiff can recover for damage or loss, the argument continues, loss cannot exist without damage in the first instance. In other words, because loss must attach to something, failing to show damage precludes recovery from loss. The Court, however, is not persuaded that Plaintiff cannot show loss.

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), provides for a civil remedy when a plaintiff "suffers damage *or* loss by reason of a violation of this section." (Emphasis added.) Here, Plaintiff's complaint alleges only loss, not damage. Under the CFAA, "loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). But courts in this district have disagreed on the question of whether loss can exist without showing damage to computer systems or interruption in service.

In *Cassetica Software Inc. v. Computer Science Corp.*, No. 09 C 0003, 2009 U.S. Dist. LEXIS 51589, (N.D. Ill. June 18, 2009), the court explained that any

“alleged loss must relate to the investigation or repair of a computer system following a violation that caused impairment or unavailability or data.” *Id.* At issue were lost fees that the plaintiffs could have received from the defendant’s downloading of the software in question. Such lost fees, the court explained, fell outside the scope of the CFAA. *Id.* (“Because Cassetica has not alleged that it lost revenues as a result of an interruption in service caused by CSC, its claim for lost revenue falls outside the statutory definition of ‘loss.’”).

The reasoning of the *Cassetica* court was followed in *CustomGuide v. CareerBuilder, LLC*, 813 F. Supp. 2d 990 (N.D. Ill. 2011). There, “[d]espite not having a license for business-to-business sales of CustomGuide’s content, CareerBuilder made unauthorized access to CustomGuide’s system and used CustomGuide’s content for business-to-business sales.” *Id.* at 995. CustomGuide argued that such unauthorized use amounted to CFAA loss. But the court disagreed, noting that “lost revenues that are not related to the impairment of a computer system are not recoverable under the CFAA.” *Id.* at 998.

This reasoning was also endorsed in *von Holdt v. A-1 Tool Corp.*, 714 F. Supp. 2d 863 (N.D. Ill. 2010) (rejecting the argument that “loss does not require an interruption of service or damage to the computer or computer system”). At issue in that case was the allegedly unauthorized access of confidential files, which allegedly resulted in the sharing of confidential information. *Id.* at 874. Although the plaintiff had no problems accessing or using their system, they still hired a forensic computer expert in response. *Id.* at 875. But the court held that insufficient because

the alleged loss did not stem from unavailability of data or a service interruption. *Id.* It noted that “because the plaintiffs have failed to point to any evidence establishing that their computers were impaired or that they suffered an interruption of service, the CFAA claim fails on this ground.” *Id.*

Other courts in the Seventh Circuit have seemed to reject that reasoning. In *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, the court summarily noted that “the majority view in this district is that ‘a plaintiff can satisfy the CFAA’s definition of loss by alleging costs reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused no damage as defined by the CFAA.’” 364 F. Supp. 3d 888, 907 (N.D. Ill. 2019) (quoting *PolyOne Corp v. Lu*, No. 14 CV 10369, 2018 U.S. Dist. LEXIS 167482, at *43 (N.D. Ill. Sept. 28, 2018)). The *Abrasic* court followed the view of the *PolyOne* court, but neither provided any reasoning on the point.

In finding such a “majority” holding, the *PolyOne* court was following the reasoning in *Farmers Insurance Exchange v. Auto Club Group*, in which the court noted the lack of consistency among the decisions of the district courts within the Seventh Circuit. 823 F. Supp. 2d 847, 854 (N.D. Ill. 2011) (“District courts within this circuit have interpreted this language in different ways.”). But the *Farmers Insurance* court never said there was a majority view. It did, however, disagree with the *Cassetica Software* line of cases when it held that “a plaintiff can satisfy the CFAA’s definition of loss by alleging costs reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused

no damage as defined by the CFAA.” *Id.* at 854–55. Notably, this is the sentence that subsequent courts relied on.

But in disagreeing with the *Cassetica Software* line of cases, the *Farmers Insurance* court seemed to make a nuanced distinction. For example, the court distinguished *Mintel v. Neergheen*, No. 08 C 3939, 2010 U.S. Dist. LEXIS 2323, at *33 (N.D. Ill. Jan. 12 2010) on the grounds that the purported loss was the cost of an expert that was hired for assistance in the lawsuit instead of to directly respond to a CFAA violation. *Farmers Insurance*, 823 F. Supp. 2d at 855. Furthermore, the court agreed with prior cases that “costs not related to computer impairment or computer damages are not compensable under the CFAA.” *Id.* Thus, *Farmers Insurance* seems to stand for the proposition that, although plaintiffs are not required to allege or show cognizable CFAA damage, the purported loss still must be related to computer impairment or computer damage in some way. In doing so, *Farmers Insurance* seems to be crawfishing from its rejection of *Cassetica Software*. This reading of *Farmers Insurance* is bolstered by the next paragraph of the opinion.

To the extent Farmers has claimed costs incurred as a result of “determining and complying with customer security breach notification obligations as required by the laws of the States in which the affected customers reside,” the loss of “present and future business,” and damages to its reputation, the court finds that these allegations do not satisfy the CFAA’s definition of loss. These losses are not directly attributable to Auto Club’s unauthorized computer access itself, but are instead properly attributable to the resulting disclosure of certain confidential information to Auto Club personnel and Auto Club’s subsequent use of Farmers’ confidential policyholder information to Farmers’ detriment. As such, these damages “are better addressed, as they are here, under . . . trade secrets law.”

Id. at 855–56 (quoting *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009)). Thus, under *Farmers Insurance*, the analysis of whether the purported loss qualifies as CFAA loss seems to be a matter of determining the level of attenuation from the alleged violation of the CFAA. If the loss is not so attenuated that it falls outside the scope of the CFAA, the plaintiff will be able to recover those losses after it proves a CFAA violation on the merits. By way of a hyperbolic example, victims could not claim “loss” under the CFAA because they lost sleep over a violation and, consequently, purchased a sensory deprivation chamber to get some shut eye.

To the extent the *Cassetica Software* line of cases, and even those parts of *Farmers Insurance*, require damage—be they “damage” under the CFAA or traditional tort type of damages—the Court respectfully parts company. “Loss” and “damage” are distinct in the CFAA. Indeed, each term has its own distinct definition. 18 U.S.C. §§ 1030(e)(8), (11). And “loss” is broadly defined. So, the scope of “loss” cannot be limited by engrafting either the CFAA’s statutory definition of “damage” or the common-law definition of “damage” onto the term. The plain language of the statute does not allow for that construction: “[T]he term ‘loss’ means any reasonable cost to any victim. . .” 18 U.S.C. §1030(e)(11). As can be seen, “loss” is defined by referencing “costs” to the victim. So, “cost” limns the concept of “loss” in the CFAA. “Costs” are expenditures to address or remedy the violation, which has a reasonable causal connection.

Here, much of Plaintiff's purported loss falls outside the scope of the CFAA. These items are simply not "costs." Plaintiff alleges that they have lost at least 134 customers because they have switched to Defendant JobProgress's product. Dkt. 178, ¶ 50. Plaintiff has not put forth evidence showing why those customers made the switch. Even crediting all reasonable inferences in Plaintiff's favor, this is not sufficient to show a connection to the alleged violation of the CFAA. Furthermore, even if the 134 customers switched to JobProgress because of Defendants' purported misuse of confidential information, that would still be too far attenuated from Defendants' password sharing⁵ to constitute loss. Plaintiff also alleges that it lost revenues from licensing fees that it would have charged if not for Defendants' actions. *Id.* ¶ 51. But like the lost fees in *Cassetica Software*, these lost licensing fees fall outside the scope of the CFAA.

Plaintiff's CEO Michael Stein also testified at his deposition regarding the loss suffered as a result of Defendants' actions. Dkt. 160-23. He explained that Plaintiff realized JobProgress was "a blatant rip-off of Acculynx" after JobProgress, LLC presented its software at a trade show in Las Vegas. Dkt. 160-23, ¶ 2. Because Plaintiff did not yet know how its software was allegedly ripped off, it formed a "team to conduct a damage and security assessment." *Id.* ¶ 7. This included over \$5,000 in fees paid to Plaintiff's legal counsel and \$2,200 paid to Yaniv Schiff to review the technical aspects of Defendants' actions. *Id.* ¶ 12. Plaintiff also asserts loss in excess of \$13,000 for time spent by its own employees. *Id.* ¶ 14. Much of

⁵ To be clear, the Court makes no determination regarding whether Defendants' password sharing constitutes a CFAA violation.

these costs are insufficient as too attenuated from the alleged CFAA violation, but others are not.

The purported loss must have a reasonable causal connection to the CFAA violation, instead of costs associated with the loss of confidential information or preparation for litigation as discussed in *Mintel* and *Farmers Insurance*. Thus, to the extent that Plaintiff's legal costs relate to this litigation, they are simply too attenuated to qualify as CFAA loss. But to the extent that Plaintiff's legal costs result from responding to the offense or conducting a damage assessment, those would constitute "loss" because there is a reasonable causal connection.⁶

Plaintiff has shown legal fees and cost of employee salary well above the \$5,000 threshold. But these costs calculations did not differentiate between costs related to the damage assessment and costs related to the subsequent litigation. Still, given the dollar figure of the cost involved, the Court credits Plaintiff with the reasonable inference that in the end, the loss is greater than \$5,000. This is especially true because the \$2,200 paid to Mr. Schiff for the technical damage is squarely within the definition of CFAA loss.

Because Plaintiff can show sufficient loss, the Court denies Defendants' motion for summary judgment on Plaintiff's Computer Fraud and Abuse Act claim.

3. Plaintiff's motion for summary judgment on its CFAA claim

⁶ By way of example, legal fees paid to attorneys charged with supervising an incident response investigation to determine what wrongdoing occurred might be sufficiently related to the CFAA violation. On the other hand, legal fees to prepare for the resulting litigation, would be too far attenuated.

Plaintiff has also moved the Court for summary judgment on its CFAA claim. But Plaintiff does not effectively develop the argument. Plaintiff's brief merely recites the statutory language and concludes that Defendants' actions qualify. Plaintiff fails to cite to any case in which password sharing was held to be a violation of the CFAA. Plaintiff fails to argue for a reasonable extension of the law based on analogous reasoning, or any reasoning. Plaintiff merely assumes that the facts at hand constitute a violation. Thus, Plaintiff has failed to meet its burden of persuasion, and its motion for summary judgment on the CFAA claim is denied.

B. Preemption of common law claims

Counts IV, VI, VII, and VIII of Plaintiff's complaint allege fraud, unjust enrichment, conspiracy, and unfair competition. Dkt. 100, ¶¶ 70–76, 83–95. Defendants contend that all of these claims are preempted by the Illinois Trade Secrets Act (ITSA). Dkt. 146, at 5–7.

The Illinois Trade Secrets Act explicitly states that it “is intended to displace conflicting tort, restitutionary, unfair competition, and other laws of this State providing civil remedies for misappropriation of a trade secret.” 765 Ill. Comp. Stat. 1065/8 (West 1994). At bottom, all common law claims based on misappropriation of trade secrets were codified, and preempted, by ITSA. *Thomas & Betts Corp. v. Panduit Corp.*, 108 F. Supp. 968, 971–72 (N.D. Ill. 2000); *Pope v. Alberto-Culver Co.*, 694 N.E.2d 615, 619 (Ill. App. Ct. 1998). This extends to confidential information, even where such confidential information does not actually fall within ITSA's statutory definition of a trade secret. *Cronimet Holdings, Inc. v. Keywell Metals*,

LLC, 73 F. Supp. 3d 907, 920 (N.D. Ill. 2014) (citing *Spitz v. Proven Winners N. Am.*, 759 F.3d 724, 733 (7th Cir. 2014)). In deciding the preemption issue, courts need not determine whether the alleged trade secret is in fact a trade secret. Courts merely assess whether the common law claim is based on the misappropriation of an alleged trade secret. As the Seventh Circuit explained in *Composite Marine Propellers, Inc. v. Van Der Woude*, “[u]nless defendants misappropriated a (statutory) trade secret, they did no legal wrong.” 962 F.2d 1263, 1265 (7th Cir. 1992).

Still, for preemption to exist, the common law claim must be based on the misappropriation of allegedly confidential information or trade secrets. *Hecny Trans. Inc. v. Chu*, 430 F.3d 402, 404–05 (7th Cir. 2005) (accepting the “dominant view” that “claims are foreclosed only when they rest on the conduct that is said to misappropriate trade secrets”). “The pertinent question[] then is whether those claims would stand even if the [information] was not alleged to be a trade secret.” *Am. Ctr. for Excellence in Surgical Assisting, Inc. v. Cmty. Coll. Dist.* 502, 190 F. Supp. 3d 812, 823 (N.D. Ill. 2016). In other words, is the claim based on misappropriation, or does the plaintiff seek redress “for wrongs beyond the mere misappropriation”? *Id.* (quoting *Charles Schwab & Co. v. Carter*, No. 04 C 7074, 2005 U.S. Dist. LEXIS 21348, at *4 (N.D. Ill. Sept. 27, 2005)). For example, in *American Center for Excellence in Surgical Assisting, Inc.*, the plaintiff alleged the misappropriation of a trade secret but also that the defendant fraudulently induced them “to provide its knowledge and expertise to help build” the product. *Id.* at 825.

Given that, the Court determined that plaintiff's complaint would state a claim for fraud even without the misappropriation of a trade secret. Thus, the Court held that ITSA did not preempt the fraud claim. *Id.*

1. Fraud

Defendants claim that ITSA preempts Plaintiff's fraud claim. In contrast, Plaintiff argues that ITSA does not preempt the claim because it would exist independent of any alleged misappropriation. In support, Plaintiff cites to *CardioNet, Inc. v. Lifewatch Corp.*, No. 07 C 6625, 2008 U.S. Dist. LEXIS 15938 (N.D. Ill. Feb. 27, 2008). Indeed, that case provides a helpful distinction between what is and is not preempted. There, the plaintiff had developed a medical device that monitored a patient's heart throughout the day. *Id.* at *3. The plaintiff alleged that the defendant fraudulently obtained two of these devices to obtain confidential, proprietary, and trade secret information. *Id.* at *4–5.

The court then explained that the fraud of acquiring the physical devices themselves was different from any alleged fraud related to the acquisition of any confidential information contained within the devices. Defendants had not merely purchased the devices. They allegedly acquired them by fraudulently obtaining prescriptions. Thus, the claim of fraud based on the acquisition of the medical devices was not preempted by ITSA, but the claim of fraud based on any acquisition of confidential information or trade secrets contained within the devices was preempted. *Id.*

Here, Plaintiff argues that its fraud claim should survive summary judgment because it is independent of any alleged misappropriation of confidential information. Dkt. 167, at 10–11. But that argument is not persuasive. As part of its argument that the claim is not merely a repackaged ITSA claim, Plaintiff points to an “elaborate scheme of deception and subterfuge” that caused harm to Plaintiff “in ways that go beyond the misappropriation of [its] trade secrets.” *Id.* at 10 (quoting Dkt. 100, at ¶¶ 46, 76). Specifically, Plaintiff explains that Defendants shared their login credentials with their consultant team in India and that they cheated Plaintiff out of licensing fees in the amount of \$32,076. *Id.* Furthermore, Plaintiffs point to a scheme to obtain and capitalize on Plaintiff’s “knowledge and learning” as well as its “expertise, labor, years of hard work, monetary investment, and customer goodwill.” *Id.* at 10–11 (quoting Dkt. 179, ¶ 9; Dkt. 100, ¶¶ 4, 17, 48).

To be clear, any claim of fraud based on the misappropriation of trade secrets or confidential information is preempted. The only question is whether Plaintiff has other fraud claims that would lie independent of any confidential information. In Plaintiff’s first amended complaint, it alleges fraud based on Defendants sharing login credentials with their consultants in India and allegedly depriving Plaintiffs of licensing fees for additional users. Dkt. 100, ¶¶ 70–76. But login credentials are confidential information to protect trade secrets. If they were not confidential, then there would be no point to their existence. Additionally, Plaintiff has asserted that the information protected by the login credentials is also confidential. Furthermore, any loss of licensing fees from the sharing of such information is still based on the

misuse of confidential information. The Court sees no claim for fraud that could be brought independent of the existence of any confidential information. Thus, on the limited question of preemption of the fraud claim, summary judgment is granted to Defendants.

2. Unjust Enrichment

Defendants also assert that ITSA preempts Plaintiff's unjust enrichment claim. The argument here is duplicative of the argument above. Plaintiff responds in a similar fashion, but also cites to *IPOX Schuster, LCC v. Nikko Asset Mgmt Co.*, 191 F. Supp. 3d 790 (N.D. Ill. 2016). Based on this case, Plaintiff contends that "portions of the unjust enrichment claim [] do not depend solely on the misappropriation of trade secrets" and thus it should survive summary judgment. Dkt. 167, at 12.

In *IPOX Schuster*, the defendants had repeatedly asked IPOX about how their product functioned, even after defendants launched their product. *Id.* at 5–8. When defendants launched their product, they did so without obtaining a license from IPOX, even though the product was allegedly based on and used IPOX's product. *Id.* at 7–8. Furthermore, the defendants in that case had advertised to its customers that it used IPOX's product and even displayed their trademark. *Id.* at 7. Thus, the defendants in that case allegedly used IPOX's reputation, goodwill, skills, and expertise to further their own business venture. *Id.* The *IPOX* court found that "[p]ortions of IPOX's unjust enrichment and common law misappropriation claims [were] based on the misuse of IPX's trademark, reputation, and goodwill" and were

not based on confidential information or trade secrets. Therefore, the *IPOX* court held that ITSA did not preempt those claims. *Id.* at 22–23.

Although we are at the summary judgment stage, the Court still looks at the complaint to determine Plaintiff's claims. *Bartholet v. Reishauer A.G.*, 953 F.2d 1073, 1078 (7th Cir. 1992). Under its claim for unjust enrichment, Plaintiff includes the typical language about incorporating all the previous paragraphs of the complaint into the unjust enrichment count. Dkt. 100, ¶ 83. But Plaintiff also explains that the claim is based on Plaintiff's "confidential information that does not meet the statutory definition of a trade secret." *Id.* ¶ 84. Plaintiff does not go further to make claims outside of the use of such confidential information. *Id.* ¶¶ 83–86. As stated above, preemption applies to both trade secrets and otherwise confidential information. Because Plaintiff's claim for unjust enrichment is based on such information, it is preempted.

Plaintiff's citation to *IPOX* does not repair the problem. Unlike in *IPOX*, Defendants here did not continually ask Plaintiff questions about how the software worked. Defendants did not rely on Plaintiff's expertise. Defendants did not display Plaintiff's trademark or otherwise attempt to benefit from Plaintiff's goodwill and reputation in the industry. *IPOX* is simply not analogous to the present case. Because Plaintiff's claim for unjust enrichment is based on Defendants' use of any confidential information, it is preempted and summary judgment in favor of Defendants on that claim is granted.

3. Conspiracy

Defendant next argues that ITSA also preempts Plaintiff's claim for conspiracy. Plaintiff alleges that "Defendants combined to commit the previously described tortious acts, which they carried out in an effort to compete with plaintiff." Dkt. 100, ¶ 88. In the immediately preceding paragraph, which begins the section describing the conspiracy count, Plaintiff incorporates all previous allegations in the complaint. *Id.* ¶ 87. Reading the complaint generously, the Court finds that Plaintiff claims a conspiracy as to the Defendant's entire operation, which thus encompasses all claims. Although the complaint describes "tortious" acts—implying common law claims—it can also be reasonably read to imply a larger conspiracy that includes the CFAA claim, the ITSA claim, and the breach of contract claim.

Duplicative legal analysis is unnecessary here. The same reasoning applies. ITSA preempts common law claims based on confidential information or trade secrets. ITSA does not preempt any remaining claims that could have been brought independent of any misappropriation of confidential information or trade secrets. Thus, to the extent Plaintiff claims conspiracy to commit common law fraud, unfair competition, or to be unjustly enriched by those actions, the claims are preempted, and summary judgment is granted to Defendants. But to the extent that Plaintiff claims a conspiracy to violate the CFAA, that claim cannot be preempted by any state law. Likewise, ITSA expressly does not preempt contract claims. 765 ILCS 1065/8(b)(2). Thus, any conspiracy claims that attach to the CFAA, the breach of

contract claim, or the purported ITSA violation survive Defendants' motion for summary judgment.

4. Unfair Competition

Just like above, Defendants again contend that Plaintiff's unfair competition claim is preempted. Just as with the unjust enrichment claim, Plaintiff's complaint again alleges that the unfair competition claim is "based upon [Plaintiff's] confidential information that does not meet the statutory definition of a trade secret." Dkt. 100, ¶ 91. But here again, Plaintiff incorrectly assumes that only information that meets the ITSA statutory definition is preempted. As previously noted, the confidential information at issue here is also subject to preemption, and because Plaintiff's common law unfair competition claim is based on that confidential information, ITSA preempts it. If Plaintiff's injuries based on misappropriation of trade secrets or confidential information are redressable, such remedies must be found in the Illinois Trade Secrets Act.

Plaintiff responds that its unfair competition claim is not preempted because Defendants "intentionally and wrongfully misappropriated the labors and financial expenditures of [Plaintiff] through fraud or deception." Dkt. 167, at 13 (quoting Dkt. 100, ¶ 93). In support of this distinction, Plaintiff cites to *Segerdahl v. Ferruzza*, No. 17-cv-3015, 2019 U.S. Dist. LEXIS 492, at *6 (N.D. Ill. Feb. 10, 2018), but that case does not discuss preemption as it relates to unfair competition. It, therefore, is not persuasive. Instead, *Thomas & Betts Corp. v. Panduit Corp.*, is instructive. 108 F. Supp. 2d 968, 973–74 (N.D. Ill. 2000). There, the plaintiff asserted the following:

[D]efendants used the confidential information to attempt to convert T&B's distributor sales; make inroads into the MRO market and convert T&B's sales to distributors and end-users in that market; develop Panduit's Barb-Ty product and convert T&B's Signature Service Program; and develop and implement Panduit's Delta, PEP and CEP programs to convert T&B's sales.

Id. at 973. In other words, plaintiff's allegations merely described how "defendants used the confidential information taken" from them. *Id.* Thus, the unfair competition claim was preempted by ITSA. *Id.*

Here, Plaintiff's unfair competition claim suffers the same fate. Plaintiff claims that it "invested substantial capital, labor, and time in creation and development" of its product. Dkt. 100, ¶ 92. But what trade secrets do not require such expenditures? This is nothing new and does not change the preemption analysis. Just as in *Thomas & Betts*, Plaintiff's unfair competition claim is based on confidential information that Defendants allegedly misappropriated. All Plaintiff has done is restate what Defendants did with the information. Therefore, ITSA preempts Plaintiff's unfair competition claim and summary judgment on that claim is granted to Defendants.

Having discussed each of Defendants' preemption claims, the Court reiterates that Defendants' motion for summary judgment as to Counts IV, VI, VII, and VIII is granted—with the exception that any conspiracy claim based on breach of contract, ITSA, or the CFAA survives Defendants' motion.

IV. Illinois Trade Secrets Act

Defendants also move for summary judgment on Plaintiff's claim under the Illinois Trade Secrets Act (ITSA). ITSA provides a statutory definition of a trade secret:

“Trade secret” means information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or supplies that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

765 ILCS 1065/2(d). Defendants claim they are entitled to summary judgment because Plaintiff did not sufficiently maintain the secrecy of its alleged trade secrets as required by § 1065/2(d)(2). Dkt. 146, at 18. Predictably, Plaintiff believes it adequately protected the alleged trade secrets and also responds that Defendants have misstated the law. Dkt. 167, at 28–35.

The parties disagree over the extent to which summary judgment is appropriate when determining whether reasonable steps were taken to maintain the secrecy of information. To be sure, such questions are ordinarily the province of the fact finder. *CMBB LLC v. Lockwood Mfg.*, 628 F. Supp. 2d 881, 883–84 (N.D. Ill. 2009) (quoting *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.* 342 F.3d 714, 725 (7th Cir. 2003)). Still, in the rare ITSA case in which the Court can determine that no reasonable jury could find for the nonmovant, summary judgment is still appropriate. Thus, this Court will only grant summary judgment if the record clearly indicates that reasonable measures to maintain the secrecy of the

information in question “simply were not taken.” *Id.* at 884 (quoting *Tax Track Sys. Corp. v. New Investor World, Inc.*, 478 F.3d 783, 787 (7th Cir. 2007)).

To set the stage, discussion of a couple of relevant prior cases is warranted. In *CMBB*, the court determined that the facts presented were that rare case that warranted summary judgment in favor of the defendant. *Id.* There, the information in question was “customer names, contacts, telephone numbers, product purchases, pricing and amounts paid.” *Id.* at 883. Essentially, the information appears to have been used by salespersons to generate business, including a defendant Jennifer Bryan. On her exit from the company, Bryan was permitted to keep her laptop without removing any of the customer information and purportedly used the customer information when she was eventually hired by Lockwood Manufacturing, the other defendant in the case. *Id.* at 885. Beyond permitting Bryan to keep her work laptop, the company failed to tell its employees that the customer information was a trade secret, or even confidential. *Id.* at 885. Nor did they have written agreements or policies limiting its use. *Id.* Furthermore, the information was sold from Chicago Metallic to CMBB, but CMBB failed to require that Chicago Metallic destroy its copies of the information or to require its employees to stop using it. *Id.* at 884. Thus, the Court determined that no reasonable jury could find that the plaintiff had taken reasonable steps to treat the information as secret.

In *Geraci v. Amidon*, an Illinois appellate court determined that the efforts to maintain secrecy were reasonable under the circumstances. No. 2-12-0023, 2013 IL App (2d) 120023-U, at *51 (Ill. App. Ct. Dec. 23, 2013). Those measures included

“password protection, security tokens, security suites and network administration tools, lock[ing] the computer server in a separate room, and us[ing] employment and confidentiality agreements.” *Id.*

Here, uncontested facts exist that militate toward a finding that Plaintiff’s measures to keep its information secret were reasonable under the circumstances. Still, further uncontested facts could lead a jury to conclude otherwise. Unlike *CMBB*, Plaintiff here used seemingly strict contractual language to protect the secrecy of its product. Similar to the facts in *Geraci*, Plaintiff here used password protection to ensure only authorized subscribers had access to the software. On the other hand, Plaintiff also displayed its product at trade shows and during other sales presentations. Beyond that, Plaintiff’s sales staff were not given instructions to limit the scope of their presentations to protect the confidentiality of the software. Thus, favorable facts exist for both sides of this debate. The question, therefore, is best left to a jury to answer. The motion for summary judgment on Plaintiff’s ITSA claim is denied.

V. Breach of Contract

A. Who are the parties to the contract?

As an initial matter, Defendants argue that the only party to the contract with Plaintiff is Double D Construction.⁷ Defendant JobProgress, LLC, the argument continues, did not exist at the time that the contract was formed, and

⁷ For clarity, the Court uses the word “contract” in its singular form. This includes the Master Subscription Agreement, the Training Agreement, and the Terms and Conditions of use.

David Buzzelli and Dennis Darrow were merely acting as agents of Double D Construction. Dkt. 146, at 27–28. Plaintiff counters in three ways. First, Plaintiff contends that all defendants conspired to breach the contract in question, and thus can be held liable regardless of whether they were direct parties to the contract. Second, Plaintiff argues that Darrow and Buzzelli repeatedly accessed the Acculynx software, the terms and conditions of which amount to a clickwrap agreement that made them a party to the contract. Dkt. 159, at 17–18. Lastly, Plaintiff contends that Buzzelli’s and Darrow’s actions after JobProgress was formed makes JobProgress—which is an LLC—a party to the contract because they acted on its behalf. Dkt. 159, at 14–18.

First, Plaintiff’s claim that all Defendants are parties to the contract is not persuasive. Plaintiff contends that the Defendants can all be held liable as parties to the contract because of an alleged conspiracy—an argument Plaintiff fails to develop or support with any citation to legal authority. Plaintiff’s argument could be read to simply contend that all defendants can be held liable because of a conspiracy to breach the contract—notwithstanding that they are not parties to that contract. But that is a separate claim from the breach of contract claim and its analysis is necessarily separate.

Second, Plaintiff alleges that Dennis Darrow and David Buzzelli became parties to the contract by accessing the software and agreeing to the terms and conditions. This argument is equally unpersuasive. Employees and agents of business entities access software regularly on behalf of their employers. This is

commonplace in today's technology-focused world. They do not become parties to their employers' contracts merely by carrying out the functions of their employment. Nor does Plaintiff expect this result. Plaintiff's agreement expressly differentiates between the software licensee and the licensee's employees and agents. Defendants point out that the Master Subscription Agreement states, "If you are entering this agreement on behalf of a corporation . . . the terms 'you' or 'your' shall refer to such entity and its affiliates." Dkt. 146, at 27–28. As Defendants note, this clause would make no sense if each user were agreeing to become a party to the contract directly. *Id.*

Double D Construction is the customer that entered into a subscription contract with Plaintiff. Double D Construction's employees and agents are not parties to the contract themselves, especially if they signed the contract on behalf of the company.

Lastly, as Defendants point out, JobProgress had not been formed at the time of the contract. Notably, Plaintiff has not argued that any Defendant acted as a promoter for the to-be-formed JobProgress or that JobProgress ratified any agreement once it was formed. Plaintiff does seem to argue that by using the software, Defendants made JobProgress a party to the contract. But this two-sentence argument is not persuasive. Plaintiff does not present any evidence that anyone acted as an agent of JobProgress, LLC to become a party to any contract with them. They merely state that JobProgress is a party to the contract "to the extent that [Buzzelli and Darrow] accessed Acculynx on behalf of JobProgress once

it was formed as an LLC.” Dkt. 159, at 18. Thus, the only Defendant that is a party to the contract is Double D Construction. Summary judgment on the breach of contract claim is granted to every other Defendant.

B. Is the Contract Enforceable?

Defendants next argue that the contract is, at least in part, unenforceable. Specifically, Defendants argue that the non-disclosure agreement is unenforceable because it is overly broad, and that the noncompete agreement is unenforceable because it is unduly anticompetitive. Dkt. 146, at 29–35. Plaintiff counters that Defendants mischaracterize the nature of the agreements. The language of the agreements that Plaintiff seeks to enforce is as follows:

1.4.1 You shall not (and shall not permit any User, owner, employee, independent contractor, agent, or other third party to) copy, use, analyze, reverse engineer, decompile, disassemble, translate, convert, or apply any procedure or process to the Software in order to ascertain, derive, or appropriate for any reason or purpose, the object code, source code or source listings for the Software or any other trade secret information or process contained in the Software without the prior express written consent of AccuLynx. You shall not (and shall not permit any User, owner, employee, independent contractor, agent, or other third party to) create derivative works based on the Software; copy, frame or mirror any part or content of the Software, other than copying or framing on Your own intranets or otherwise for Your own internal business purposes; access the Software in order to build a competitive product or service; or copy any features, functions or graphics of the Software without the prior express written consent of AccuLynx

1.4.3 You shall not make the Software available to any third party other than Users; and You shall not attempt to gain unauthorized access to the Software or its related systems or networks. Basically: Don't reverse engineer our source code

1.4.5 You acknowledge that the Software and all of its components are trade secrets of AccuLynx and You agree not to (and not to permit any User, owner, employee, independent contractor, agent, or other third

party to) disclose such trade secrets without AccuLynx's prior written consent.

9.8 Severability; Blue-Penciling. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be changed by the court or interpreted so as best to accomplish the objectives of the original provisions to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect

Dkt. 100, ¶ 19; Dkt. 167, at 25. Plaintiff contends that this language is enforceable and that it does not unduly restrict Defendants from competing. It merely restricts them from creating a competitive product by stealing their information. Dkt. 167, at 23 ("Nothing in the Agreements prevents, or purports to prevent, Defendants from competing with [Acculynx], as long as they do it fairly and without stealing [Acculynx's] information.").

Under Illinois law, total restraints on trade are unenforceable as against public policy because they deprive the promisor of the opportunity to earn a living and support their family. Still, partial restraints on trade are permitted if they pass a reasonableness test. *First Nat'l Assets Mgmt. v. Garzon*, No. 2016 CH 6597, 2016 Ill. Cir. LEXIS 11198, at *8 (Cir. Ct. Sept. 6, 2016). As a threshold question, courts must determine whether the restrictive covenant is accompanied by a valid contract such that the covenant was supported by consideration. *Id.* But here, none of the parties have challenged the validity of the contract. Instead, Plaintiff argues the Defendants breached the valid contract and Defendants argue that the valid contract is unenforceable. Thus, the parties have waived any argument that no valid contract existed.

The question of whether a restrictive covenant is enforceable is a question of law. *Coady v. Harpo, Inc.*, 719 N.E.2d 244, 248 (Ill. App. Ct. 1999). In *Arcor, Inc. v. Haas*, an Illinois appellate court noted that unlike employment contracts, restrictive covenants based on the sale of a business are analyzed under a less stringent test that focuses on reasonableness. 842 N.E.2d 265, 272 (Ill. App. Ct. 2005). Businesses hold more bargaining power than ordinary employees. *Id.* Here, the business-to-business software licensing agreement at issue is more akin to the sale of a business than to an employment contract because the businesses are more likely to possess equal bargaining power. Thus, only the reasonableness test will be applied.

“To be enforceable, such a covenant must be reasonable in its time limitations and its geographic scope, involve trade secrets or confidential information, and be reasonably necessary to protect a legitimate business interest of the promisee.”⁸ *Ntron, Int’l Sales Co. v. Carroll*, 714 F. Supp. 335, 337 (N.D. Ill. 1989). Factors that should be considered when determining the reasonableness of a restrictive covenant include any injury to the public, any undue hardship and whether the restraint imposed is greater than is necessary to protect business interests, the duration of the restriction, and any geographic limitation of the covenant. *See Coady*, 719 N.E.2d at 250. But courts should not hold confidentiality agreements unenforceable solely due to a lack of durational or geographic limitations. *Id.* (citing *Pepsico, Inc. v. Redmond*, 54 F.3d 12623, 1272 n.10 (7th Cir. 1995)). Furthermore, “[a]lthough

⁸ The *Ntron International* court went on to explicitly note that confidentiality agreements must pass the same reasonableness test as other restrictive covenants. *Ntron International*, 714 F. Supp. at 337.

restraint of trade is a significant concern, ‘an equally important public policy in Illinois is the freedom to contract.’” *Id.* (quoting *Prairie Eye Ctr., Ltd. v. Butler*, 713 N.E.2d 610 (Ill. 1999)).

Against this legal backdrop, the Court holds that the contract is unenforceable in part. The contract language does not unduly restrict Double D Construction’s ability to compete in the marketplace. The provision does not prevent Double D from building a similar website and attempting to siphon off Plaintiff’s customers. It prevents Double D Construction from using any confidential information—obtained by virtue of being an Acculynx customer—to build competing software based on Acculynx. Furthermore, any policy against such restraints of trade must be weighed against the policy to promote freedom to contract and against the legitimate business need to keep confidential information out of the hands of competitors. Thus, the noncompete language itself is enforceable. But the noncompete restriction is governed by the language defining the scope of confidential information.

Defendants argues that the language defining the scope of confidential information is unenforceable for overbreadth. Dkt. 173, at 27–32. Defendants point out that Plaintiff fails to cite any case in which an analogous agreement was held enforceable. While this is true, Defendants’ likewise do not cite an Illinois case in which a confidentiality agreement attached to a software sale was held unenforceable as overbroad. Still, the Court finds that this language unenforceable as overly broad in scope in that it prevents the use of publicly available information.

In *Service Centers of Chicago v. Minogue*, an Illinois appellate court held a restrictive covenant unreasonable because it defined “confidential information as essentially all of the information provided by Deliverex to Minogue ‘concerning or in any way relating’ to the services offered.” 535 N.E.2d 1132, 1137 (Ill. App. Ct. 1989). While the facts are not entirely analogous, the point is instructive. The same can be said of *Fleetwood Packing v. Hein*, No. 14 C 9670, 2014 WL 7146439 (N.D. Ill. Dec. 15, 2014). There, the court found a confidentiality agreement unenforceable because it attempted “to bar Hein from using confidential information anywhere, for any purpose, for perpetuity.” *Id.* at *8–9. But in *Allied Waste Services of North America, LLC v. Tribble*, the court held enforceable a confidentiality agreement that broadly defined confidential information. 177 F. Supp. 3d 1103, 1111 (N.D. Ill. 2016). Although the agreement was broad, it was still limited in scope. *Id.* The agreement exhaustively enumerated examples of confidential information, and it seemed to be limited to nonpublic information and trade secrets. *Id.*

Here, the confidentiality agreement is overbroad and unenforceable as written under the specific facts of this case. Like the agreement in *Service Centers of Chicago*, the agreement here does not reasonably limit the scope of covered information. It attempts to protect all aspects of Acculynx and its components, including “any features, functions, or graphics of the Software.” Although this could be sufficient in some circumstances, the provision is not reasonable when the information in question is available to large numbers of the public. Screenshots of some aspects of Acculynx are available online through a simple Google search.

Other aspects can be seen at one of the many trade shows that Plaintiff participates in. Still other aspects of the software and its components can be seen through group or personalized demonstrations, which are not subject to nondisclosure agreements. Yet the contract language would restrict this information just as equally as information that Plaintiff more clearly protects as secret. This sweeping in of all aspects of the software, even those aspects that Plaintiff's sales staff works to demonstrate to the public, is an overbroad restriction.

Therefore, the Court holds that the confidentiality agreement language defining the scope of confidential information is unenforceable. Still, the contract includes a blue-pencil provision, which allows the Court to repair the contract and prevents the nullification of the entire agreement. So, the Court modifies the contract by adding the following clause at the beginning of § 1.4.1: "Except for information generally available to the public . . ." Thus, because the Court can repair the defect in the contract, it is enforceable as modified. Defendants' motion for summary judgment on the breach of contract claim is denied. Because any restrictive covenant regarding public information—under these facts—is unenforceable, the Court must also deny Plaintiff's motion for summary judgment on the breach of contract claim. The Court leaves for the jury the question of which information is nonpublic and thus covered by the contract—a question that must be answered before determining whether Defendants breached.

VI. Conspiracy to violate the CFAA and to breach the contract

Plaintiff moves the Court for summary judgment on the issue of whether Defendants' are liable for conspiracy to violate the CFAA and to breach the aforementioned contract. Dkt. 159, at 18. The argument fails.

Plaintiff begins the argument by asserting that Defendants are vicariously liable for the tortious actions of their employees and agents. This is a curious position given that the claim is conspiracy and not vicarious liability. Furthermore, as the Illinois Supreme Court noted in *Buckner v. Atlantic Plant Maintenance*, 694 N.E.2d 565, 571 (Ill. 1998), "there can be no conspiracy between a principal and an agent."⁹ After discussing vicarious liability, Plaintiff argues that some of Defendants' actions manifest an agency relationship and some actions are those of individual actors, outside the scope of their employment. Dkt. 159, at 20–21. Seemingly, this would mean that some actions could amount to conspiracy, while others could not. Still, Plaintiff has not persuasively argued in which capacity each defendant was acting at any given time.¹⁰ Without more, that issue is best left to a jury.

Even if the Court were convinced that the individual defendants were acting outside the scope of an agency relationship, the Court would still not be in a position to grant Plaintiff's motion. The Court has not reached the merits of the CFAA claim and knows of no cases in which a federal court has deemed simple

⁹ Intracorporate Conspiracy Doctrine in a similar context is also discussed in *PolyOne Corp v. Lu*, No. 14 CV 10369, 2018 U.S. Dist. LEXIS 167482, at *41–42 (N.D. Ill. Sept. 28, 2018).

¹⁰ While Plaintiff did list some factual assertions and what Plaintiff believes those assertions imply, Plaintiff did not apply those factual assertions to any law of agency.

password sharing between a principal and an agent a violation of that antihacking law.

Next, Plaintiff attempts to transition the conspiracy to breach a contract claim into a tort claim by referencing the Restatement (Second) of Torts § 766, which describes the tort for intentional interference with performance of a contract by third persons. Dkt. 180, at 13. Although Plaintiff claimed eight total counts in its complaint, none of them referenced the claim described in § 766. *Colbert v. City of Chicago*, 851 F.3d 649, 656 (7th Cir. 2017) (quoting *Whitaker v. Milwaukee Cty.*, 772 F.3d 802, 808 (7th Cir. 2014)) (explaining that “a party may neither amend its pleadings by argument in opposition to summary judgment nor introduce new theories of liability in opposition to summary judgment”). Thus, Plaintiff’s motion for summary judgment as to the conspiracy claim is denied.

VII. Conclusion

For the reasons stated above, Plaintiff’s motion for partial summary judgment is denied and Defendants’ motion for summary judgment is granted in part and denied in part, as outlined below:

(1) Defendants’ motion for summary judgment on Plaintiff’s Computer Fraud and Abuse Act claim is denied;

(2) Plaintiff’s motion for summary judgment on the merits of the Computer Fraud and Abuse Act claim is denied;

(3) Defendants' motion for summary judgment on Plaintiff's breach of contract claim against Double D Construction is denied;

(4) Defendants' motion for summary judgment on Plaintiff's breach of contract claim against JobProgress, LLC, Dennis Darrow, and David Buzzelli is granted;

(5) Plaintiff's motion for summary judgment on the breach of contract claim is denied;

(6) Defendants' motion for summary judgment on Plaintiff's claim for violation of the implied covenant of good faith and fair dealing is granted as uncontested;

(7) Defendants' motion for summary judgment on Plaintiff's common law fraud claim is granted because the Illinois Trade Secrets Act preempted the claim;

(8) Defendants' motion for summary judgment on Plaintiff's common law unjust enrichment claim is granted because the Illinois Trade Secrets Act preempted the claim;

(9) Defendants' motion for summary judgment on Plaintiff's common law conspiracy claim is granted as to any conspiracy claim based on fraud, unjust enrichment, or unfair competition because the Illinois Trade Secrets Act preempted them;

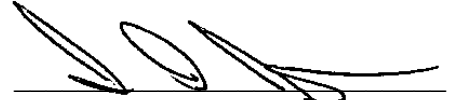
(10) Defendants' motion for summary judgment on Plaintiff's common law unfair competition claim is granted because Illinois Trade Secrets Act preempted the claim;

(11) Plaintiff's motion for summary judgment on the claim of conspiracy to commit breach of contract and to violate the CFAA is denied.

* * *

The parties are directed to contact Magistrate Judge Jensen to discuss whether a settlement conference would be appropriate at this time.

Date: December 21, 2020



Honorable Iain D. Johnston
United States District Judge